

## TA416: Activity, Techniques, & Targeting Explained | Proofpoint US

By March 07, 2022 Michael Raggi and Myrtus

Published: 2022-03-07 · Archived: 2026-04-02 11:39:01 UTC

8/24 Editor's Note: Since the publication, SMTP2Go has updated its security measures.

### Key Takeaways

- Proofpoint researchers have identified ongoing activity by the China-aligned APT actor TA416 in which the group is targeting European diplomatic entities, including an individual involved in refugee and migrant services.
- This targeting is consistent with other activity [reported](#) by Proofpoint, showing an interest in refugee policies and logistics across the APT actor landscape which coincides with increased tensions and now armed conflict between Russia and Ukraine.
- The campaigns utilize web bugs to profile the victims before sending a variety of PlugX malware payloads via malicious URLs.
- TA416 has recently updated its PlugX variant, changing its encoding method and expanding its configuration capabilities.

### Overview

Since 2020, Proofpoint researchers have observed TA416, an actor assessed to be aligned with the Chinese state, utilizing web bugs to profile their targets. Commonly referred to as tracking pixels, web bugs embed a hyperlinked non-visible object within the body of an email that, when enabled, will attempt to retrieve a benign image file from an actor-controlled server. This provides a “sign of life” to threat actors and indicates that the targeted account is valid with the user being inclined to open emails that utilize social engineering content. TA416 has been using web bugs to target victims prior to delivering malicious URLs that have installed a variety of PlugX malware payloads. The operational tempo of these campaigns, specifically those against European governments, have increased sharply since Russian troops began amassing on the border of Ukraine.

The use of the web bug reconnaissance technique suggests TA416 is being more discerning about which targets the group chooses to deliver malware payloads. Historically, the group primarily delivered web bug URLs alongside malware URLs to confirm receipt. In 2022, the group started to first profile users and then deliver malware URLs. This may be an attempt by TA416 to avoid having their malicious tools discovered and publicly disclosed. By narrowing the lens of targeting from broad phishing campaigns to focus on targets that have proven to be active and willing to open emails, TA416 increases its chance of success when following up with malicious malware payloads.

### What's In a Web Bug – Delivery in 2020 and 2021

Starting in early November 2021, Proofpoint researchers identified web bug reconnaissance campaigns targeting European diplomatic entities. Notably this activity aligned with the escalation of tensions between Russia, Ukraine, and, by extension, NATO member states in Europe. The emails first originated from a spoofed sender that impersonated a Meetings Services Assistant at the United Nations General Assembly Secretariat. Proofpoint did not observe these campaigns targeting the United Nations (UN), but did observe the targeting of diplomatic entities in Europe under the pretense of communicating with the UN. The threat actor achieved this impersonation by utilizing the legitimate email marketing service SMTP2Go, which allows users to alter the envelope sender field while using a unique sender address generated by the service.

TA416 has used SMTP2Go to impersonate various European diplomatic organizations since at least 2020. The threat actor in an August 2020 campaign impersonated the same Meetings Services Assistant at the UN General Assembly and again targeted governmental entities in Europe. In this historical campaign, TA416 delivered a DropBox URL that delivered a PlugX variant aligning with Recorded Future's [analysis](#) of "Red Delta" PlugX malware. Proofpoint assesses that there is sizeable overlap between the entities TA416 and the publicly disclosed group "Red Delta." Both campaigns from August 2020 and November 2021 targeted European diplomatic entities and utilized SMTP2Go to impersonate an external diplomatic organization that may communicate with the end targets. Included below is a publicly available malicious Zip file hash from August 2020 delivered via a DropBox URL which is attributable to TA416/Red Delta.

- Advance version of the 2020 Report of the Secretary-General on Peacebuilding and Sustaining Peace .zip | 0e3e47697539f1773fb53114ab53229c0304d86ed35aec05e5f5bfd3bd35f9a

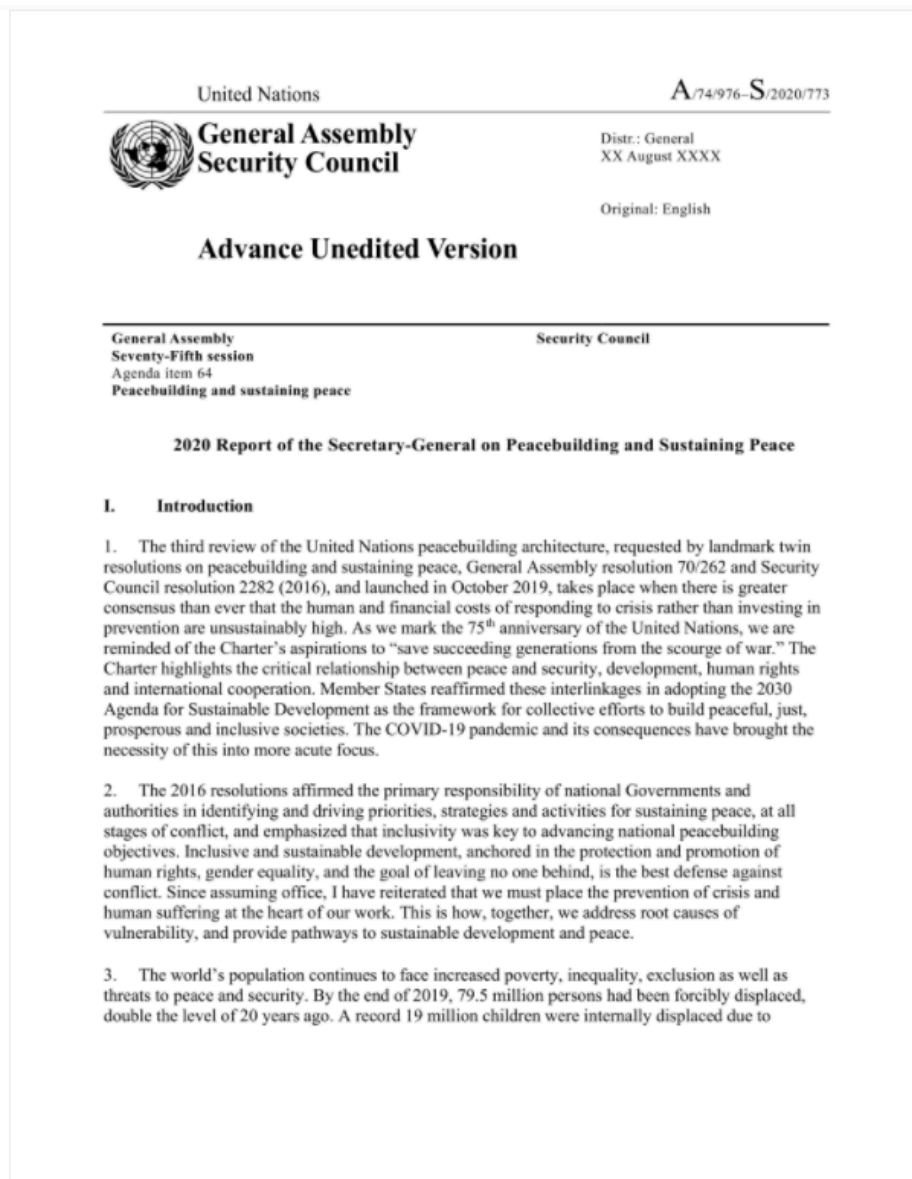


Figure 1. TA416 August 2020 “Advance version of the 2020 Report of the Secretary-General on Peacebuilding and Sustaining Peace” PDF decoy 54b491541376bda85ffb02b9bb40b9b5adba644f08b630fc1b47392625e1e60a.

### From Web Bugs to PlugX

Proofpoint researchers continued to identify web reconnaissance campaigns in November and December 2021 that utilized a rudimentary style of encoding and resource names. Fundamentally, a web bug URL includes infrastructure that hosts a benign image file, several designations about the email campaign, which can include date and campaign name, and a unique designation for each individual user targeted in the email campaign. This allows a threat actor to validate which recipients received and opened the phishing email. TA416 web bugs appear rudimentary while demonstrating slight evolution over time. The web bug URL structure began with an actor-controlled IP which retrieved jpg resources named after the email aliases of the targeted victims from the actor-controlled servers. Proofpoint researchers next observed base64 encoded values of the entire email address.

Example:

- `hxxp://45.154.14[.J235/jdoe.jpg`
- `hxxp://45.154.14[.J235/amRvZUBwcm9vZnBvaW50LmNvbQ==/328.jpg`

Researchers identified the same method of base64 encoded target emails, including in the web bug URL, consistently from August to November 2020 in TA416 campaigns that preceded the delivery of PlugX malware. On more than one occasion in 2020, this web bug technique appeared in an email alongside a Dropbox URL that ultimately delivered the Trident Loader variant of PlugX malware. [Proofpoint](#), [Avira](#), and [Recorded Future](#) have publicly attributed this installation technique to TA416/Red Delta. In the above referenced campaign from August 2020 in which TA416 impersonated UN personnel, the

threat actor utilized base64 encoded web bug resources representing targeted emails alongside the cloud hosted URLs that delivered PlugX malware. Actor-controlled IPs observed during web bug reconnaissance campaigns during the November to December 2021 period included the IP 45.154.14[.]235.

Beginning on January 17, 2022, Proofpoint researchers observed TA416 threat actors utilizing the IP address 45.154.14[.]235 in phishing emails attempting to deliver a malicious Zip file to European Diplomatic entities. These entities had previously received web bug URLs in phishing emails during the prior months. Rather than the emails delivering further reconnaissance URLs, this IP now attempted to deliver malicious Zip files. The phishing email also included a Dropbox URL attempting to deliver the same malicious archive file. Like historical TA416 campaigns, the Zip file had a geopolitically themed title, which was shared with a PDF decoy that would be later downloaded as part of the infection chain. For example, the campaign on January 17, 2022 included the following Zip and PDF file titles:

- State\_aid\_\_Commission\_approves\_2022-2027\_regional\_aid\_map\_for\_Greece.zip
- State\_aid\_\_Commission\_approves\_2022-2027\_regional\_aid\_map\_for\_Greece.pdf

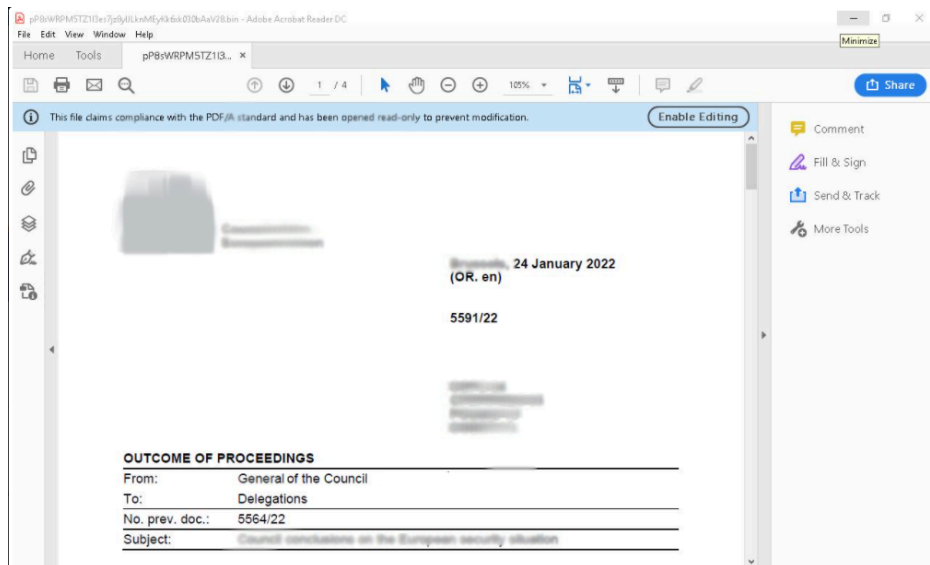


Figure 2. TA416 January 2021 PDF decoy - EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip.

While historically TA416 has delivered Zip files from cloud hosting providers containing a decoy file, legitimate PE file, a DLL loader, and a PlugX malware configuration DAT file, recent campaigns used a different tactic. Proofpoint researchers noted that the malicious Zip files delivered from DropBox now contain a rudimentary executable which is a dropper malware. This malware establishes persistence for a legitimate executable file used in DLL search order hijacking, as well as initiates the download of four components. These components are included below and resemble the components used in the past to install PlugX malware. Public research has previously documented TA416's propensity for including PlugX Trident Loader components and decoy in the initial delivered Zip file. Actors in recent months use a more convoluted delivery chain, in which a PE dropper is used to retrieve the Trident Loader components from an actor-controlled resource. The method of installing PlugX via DLL Search Order hijacking that displays a PDF decoy remains constant.

#### Requests Resulting from the Execution of Malware Dropper Executable

- PDF Decoy File

hxxps://45.154.14[.]235/State\_aid\_\_Commission\_approves\_2022- 2027\_regional\_aid\_map\_for\_Greece.pdf

- Legitimate PotPlayer PE file used in DLL Search Order Hijacking

hxxps://45.154.14[.]235/PotPlayer.exe

- Malicious PlugX Malware Loader

hxxps://45.154.14[.]235/PotPlayer.dll

- PlugX Malware Configuration Executed by DLL Search Order Hijacking

hxxps://45.154.14[.]235/PotPlayerDB.dat

Most recently on February 28, 2022, TA416 began using a compromised email address of a diplomat from a European NATO country to target a different country's diplomatic offices. The targeted individual worked in refugee and migrant services. The below URL was sent in a phishing email and delivered a compressed archive containing a PE dropper. This

dropper similarly called out to an actor-controlled URL to deliver a decoy document and the components of an updated Trident Loader PlugX malware payload.

- [hxxp://www.zyber-i\[.\]com/europa/2022.zip](http://hxxp://www.zyber-i[.]com/europa/2022.zip)
- Situation at the EU borders with Ukraine.zip|8a7fbafe9f3395272548e5aadeb1af07baeb65d7859e7a1560f580455d7b1fac
- Situation at the EU borders with Ukraine.exe|effd63168fc7957baf609f7492cd82579459963f80fc6fc4d261fbc68877f5a1(Stage 1 Dropper)
- [hxxp://103.107.104.19/2022/eu.docx](http://hxxp://103.107.104.19/2022/eu.docx) (Decoy Document)
- [hxxp://103.107.104.19/FontEDL.exe](http://hxxp://103.107.104.19/FontEDL.exe) (PE Legit)
- [hxxp://103.107.104.19/DocConvDll.dll](http://hxxp://103.107.104.19/DocConvDll.dll) (DLL Loader)
- [hxxp://103.107.104.19/FontLog.dat](http://hxxp://103.107.104.19/FontLog.dat) (PlugX Encrypted Payload)

### Communicates with C2

- [hxxps://92.118.188\[.\]78/](https://92.118.188[.]78/)

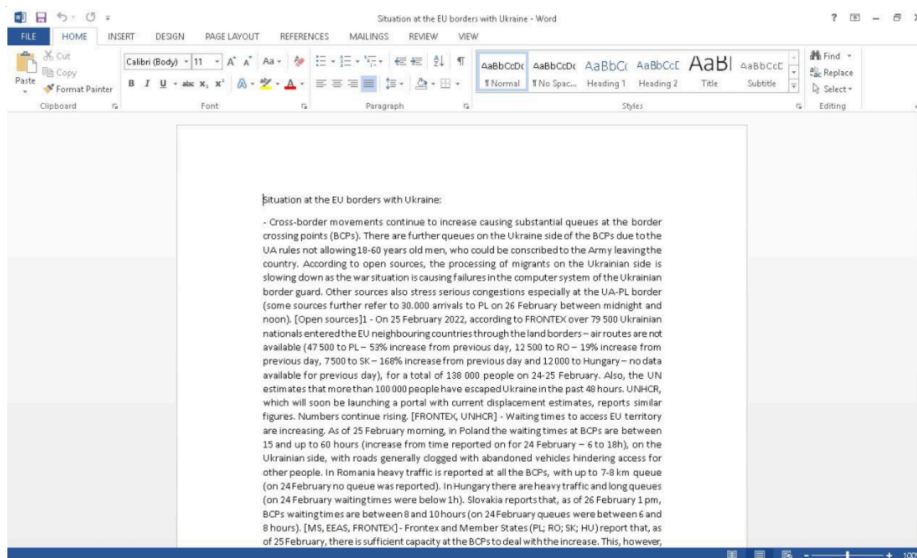


Figure 3. TA416 February 28, 2022 Word document decoy – eu.docx.

### A More Discerning Breed of TA416 PlugX Malware

Close analysis of the delivered payloads and legitimate resources retrieved from URLs by the first stage malware dropper reveals that TA416 is once again using an updated version of PlugX malware to target their victims. Historically, the group has relied on a variety of legitimate antivirus files, including the Avast file resource `wsc_proxy.exe`, to begin the process of DLL search order hijacking that results in PlugX malware installation. In the January 2022 campaigns, TA416 used the PE file `potplayermini.exe` to initiate DLL search order hijacking. This is a legitimate executable file that is part of the publicly available media player Daum PotPlayer 1.5.29825, which Mandiant has previously [documented](#) as being susceptible to search order hijacking since at least 2016. [Numerous Chinese APT groups](#), which are not directly correlated to TA416, have utilized it since that time. This campaign leveraged the vulnerability of `potplayermini.exe` to load the file `PotPlayerDB.dll` which contains an obfuscated launcher that in turn executes the file `PotPlayerDB.dat`. The file `DocConvDll.dll` has also intermittently been used as a loader of the PlugX DAT configuration files. For those that are familiar with TA416's historic tactics, techniques, and procedures (TTPs), this is highly similar to the Trident Loader method which the group used to install PlugX in previous campaigns.

While `PotPlayerDB.dat` is a variant of PlugX malware, TA416 has updated the payload by changing both its encoding method and expanding the payload's configuration capabilities. Historically, TA416 relied on the DLL launcher to decode the PlugX payload utilizing an XOR key included at the offset 0 within the PlugX DAT configuration file. In this case, TA416 has abandoned that approach in favor of something with less dependencies that is more convoluted. The latest version contains obfuscation to thwart analysis. One of the main ways it does this is by resolving API functions during runtime. Generally, malware loads a DLL, iterates over the set of exports of the DLL and hashes the string, looking for a matching hash. This iteration of PlugX does standard API hashing, but only to resolve the address of the functions `GetProcAddress` as well as `LoadLibrary`. Once those functions are resolved properly, it loads the rest of the functions via their text name.

```
mov esi, RuntimeResolvedGetProcAddress
test esi, esi
jnz short loc_1001B553 ; if GetProcAddress isn't resolved,
; resolve it and
; save to global

mov ecx, 0F8F45725h ; GetProcAddress hash
call APIHashing ; resolve GetProcAddress
mov esi, eax
mov RuntimeResolvedGetProcAddress, eax

loc_1001B553:
mov ecx, RuntimeResolvedLoadLibrary
mov dword ptr [esp+24h+apiName+4], 'Wypc'
mov dword ptr [esp+24h+apiName], 'rtsl' ; lstrcpyW
mov [esp+24h+apiName+8], 0
test ecx, ecx
jnz short loc_1001B583 ; if LoadLibrary isn't resolved,
; resolve it and
; save to global

mov ecx, 53B2070Fh
call APIHashing
mov ecx, eax
mov RuntimeResolvedLoadLibrary, eax

loc_1001B583:
mov eax, esp
mov dword ptr [esp+24h+kernel32+4], '23le'
mov dword ptr [esp+24h+kernel32], 'nrek' ; kernel32
mov [esp+24h+kernel32+8], 0
push eax
call ecx ; RuntimeResolvedLoadLibrary
lea ecx, [esp+24h+apiName]
push ecx
push eax
call esi ; RuntimeResolvedGetProcAddress
mov ecx, eax
mov RuntimeResolvedlstrcpyW, eax

loc_1001B5A8:
push ebx
push edi
call ecx ; RuntimeResolvedlstrcpyW
add esp, 18h
pop esi
pop edi
pop ebx
retn 8
WraplStrCpy endp
```

Figure 4. PlugX malware API hashing method.

In addition to this obfuscation attempt, most of the functions that contain the "business logic" of the malware are obfuscated with a state machine. At a high level this obscures the order of which blocks are executed within a function. It does this by maintaining a state variable with many comparisons in the function. After each block, the state variable is modified to whatever the subsequent block should be, making analysis more difficult. This sample further implements anti-analysis techniques via the malware's design. After every iteration of the state machine, the malware sample will modify the state with a XOR operation. This makes it difficult to analyze as the states are not hardcoded as the result of a function. This control obfuscation is apparent below with the highly cyclical nature of the control flow graph.

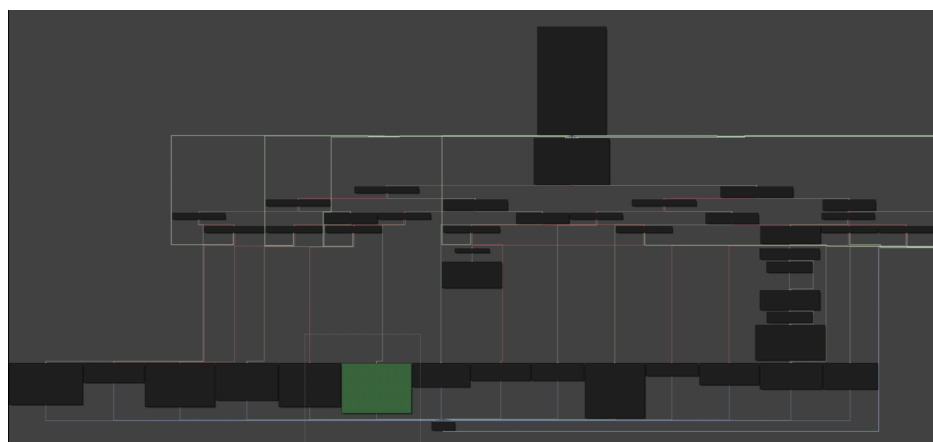


Figure 5. PlugX malware control flow graph.

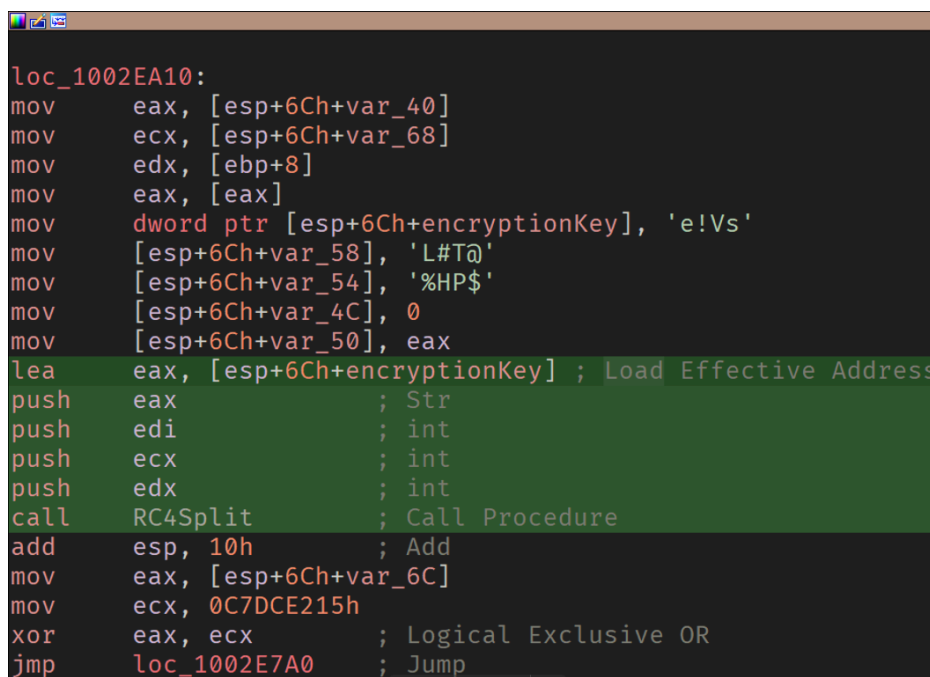
Once researchers defeated the PlugX anti-analysis techniques, they were able to examine the malware's configuration. Notably the configuration contained three additional fields that were not present in the previous versions nor in standard PlugX malware. The new version included:

- Two hardcoded dates for latest write time used to filter over files within a specified directory.
- A minimum and maximum file size to filter over files within a specified directory.
- A format string that defaults to "public/Publics" that modifies characteristics of the folder and hide it from the infected user.

In the past, when fields have been added to PlugX malware configurations they have persisted in future samples identified in subsequent campaigns. Recently, this has not always proven to be true. In recent campaigns, a consistent and clear configuration that is repeated has not been present. The expansion of the malware's configuration fields demonstrates that this tool is undergoing additional development by TA416. Further, the type of added features that enable better filtering of victim files for exfiltration and better concealment from the infected user demonstrates that the actor is going beyond anti-analysis to create a more functional and precise tool to use during intrusions. It also indicates the varying versions of the PlugX payload that are being used in a short period of time.

### Command and Control

The January 2022 version of PlugX malware utilizes RC4 encryption along with a hardcoded key that is built dynamically. For communications, the data is compressed then encrypted before sending to the command and control (C2) server and the same process in reverse is implemented for data received from the C2 server. Below shows the RC4 key "sV!e@T#LSPH%" as it is being passed along with the encrypted data. The data is compressed and decompressed via LZNT1 and RtlDecompressBuffer. During the January 2022 campaigns, the delivered PlugX malware samples communicated with the C2 server 92.118.188[.]78 over port 187. In the February 2022 campaign, Proofpoint researchers observed a variation in which PlugX malware used an RC4 key that was sent to the bot in the first HTTP response which was then used to encrypt data going to the C2 server.



```
loc_1002EA10:
mov     eax, [esp+6Ch+var_40]
mov     ecx, [esp+6Ch+var_68]
mov     edx, [ebp+8]
mov     eax, [eax]
mov     dword ptr [esp+6Ch+encryptionKey], 'e!Vs'
mov     [esp+6Ch+var_58], 'L#T@'
mov     [esp+6Ch+var_54], '%HP$'
mov     [esp+6Ch+var_4C], 0
mov     [esp+6Ch+var_50], eax
lea     eax, [esp+6Ch+encryptionKey] ; Load Effective Address
push   eax ; Str
push   edi ; int
push   ecx ; int
push   edx ; int
call   RC4Split ; Call Procedure
add     esp, 10h ; Add
mov     eax, [esp+6Ch+var_6C]
mov     ecx, 0C7DCE215h
xor     eax, ecx ; Logical Exclusive OR
jmp     loc_1002E7A0 ; Jump
```

Figure 6. PlugX malware RC4 encryption key with encrypted data.

### A Rapid Pace of Malware Development

In response to historical disclosures detailing TA416 PlugX malware infection and encoding methods, the group appears to have adopted a rapid rate of development for their PlugX payloads. While the distinctly TA416 installation method of a PE dropper retrieving Trident loaded payload components using a legitimate PE and a DLL loader file to load a PlugX payload remains constant, the components in this infection chain are regularly changing. The group uses different legitimate PE files to initiate sideloading, as well as a variety of PlugX DLL loaders including the PotPlayer and DocCon versions noted in this publication. TA416 also uses different variants of the final PlugX payload in which the communication routines are observed to be different when closely analyzed. Additionally, the payload DAT file decryption method has evolved regularly since the beginning of 2022. Several observed decryption schemas and a sample configuration are included below with date ranges detailing the evolution of observed PlugX payloads.

```
data = open(r"adobeupdate.dat.secure", "rb").read()

data_offset = data.find(b"\x00")

key = data[:data_offset]
data = bytearray(data[data_offset+1:])

for i, b in enumerate(data):
    data[i] ^= key[i % len(key)]

open("payload.bin", "wb").write(data)
```

Figure 7. 2020 - 2022 PlugX DAT file decryption.

```
def new_variant(data:bytearray):
    res = bytearray()
    modifier = 0x15DF
    for i in range(len(data)):
        modifier -= 0x36363636 & 0xFFFFFFFF
        tmp = (modifier & 0x4A | ~modifier & 0xB5) ^ (data[i] & 0x4A |
~data[i] & 0xB5)
        res.append(tmp)

    return res
```

Figure 8. January 2022 – February 2022 PlugX DAT file decryption.

```
def new_variant(data:bytearray):
    res = bytearray()
    modifier = 0xCE5
    for i in range(len(data)):
        modifier += 0x17042fc & 0xFFFFFFFF

        tmp = ((modifier & 0xff) ^ 0xff) & data[i] | (data[i] ^ 0xff) &
(counter & 0xff)
        res.append(tmp)

    return res
```

Figure 9. Mid-February 2022 PlugX DAT file decryption.

```

struct CONFIG {
    int sleepAmount; // used within WaitForSingelObject
    uint unused;
    int DesiredArchitecture; // evaluated via the following (32 or 64) &&
DesiredArchitecture = (0 or 64)
    int unused7;
    time64_t TimeWriteLowerBound; // compared against last write time
    uint64 MaxFileSize; // compared against last write time
    uint64 MinFileSize; // compared against files being read
    time64_t TimeWriteUpperBound; // compared against last write time
    char InstallDir[16]; // where the client is rewritten to be launched
via persistnece
    char unused2[112]; // null bytes
    char Mutex[24]; // mutex to create
    char unused3[104]; // null bytes
    int64 BCAStr; // something related to the strings in use
    char unused4[120];
    int str2; // used related to a docusment.exe
    char unused5[516]; // null bytes
    char PublicStr[32]; // hidden directory that's created and used to
store modules
    char unused6[488]; // null bytes

    struct C2Comms {
        short IPID; // either 1 or 6
        short Port;
        char IPStr[13];
        char unused6[179];
    } C2Array[4];
} conf;

```

Figure 10. PlugX malware configuration sample.

**Attribution**

Proofpoint researchers assess with high confidence that the operator identified in recent campaigns delivering PlugX malware is the same as previously identified in 2020 as part of Recorded Future’s Red Delta campaign. This assessment is based on the use of the same email marketing service to deliver emails, the consistent impersonation of European diplomatic entities, the repetition of web bug patterns in the 2020, 2021, and 2022 campaigns, the consistent victimology observed between the campaigns, a nearly identical file naming structure observed between Zip and PDF decoy files, and the highly similar Trident Loader TTPs used for the execution of PlugX malware.

Tactic	2020	2021 – 2022
	TA416 Campaigns	TA416 Campaigns
Spoofing Via SMPT2Go	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Impersonation of UN Personnel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Rudimentary Base64 Web Bugs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Trident Loaded PlugX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

<b>Politically Themed PDF Decoys</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Shared Zip and PDF Decoy File Names</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>Targeted European Diplomatic Entities</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 11. Mapping TA416 TTPs over time.

### Conclusion

The multiyear campaign against diplomatic entities in Europe suggests a consistent area of responsibility belonging to TA416. This mandate may have increased against entities in Europe during the current period of geopolitical conflict and economic upheaval in Europe. While historically the phishing tactics and tools of this group have not been so thoroughly explored, the consistent reliance on updating PlugX malware installation using the Trident Loader method belies a lack of innovation on the part of TA416 following several major publications surrounding this actor. TA416 has chosen to compensate for this lack of innovation with a greater tempo of variation. The group has proved to be pragmatic, making incremental and staggered changes to their PlugX toolkit rapidly and regularly altering a toolset it has used for the past number of years. Despite these variations, the group’s persistent targeting of a habitual target set paired with ingrained phishing tactics often leads to periodic discovery by threat researchers. Once TA416 reads this latest publication regarding their tactics, researchers at Proofpoint fully anticipate they will remain the metaphorical “Tubthumping” of the APT landscape. Researchers can publish their tactics but will never keep them down.

### Indicators of Compromise (IOCs)

<b>IOC</b>
<a href="https://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip">https://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip</a>
<a href="https://www.dropbox[.]com/s/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip?dl=1">https://www.dropbox[.]com/s/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.zip?dl=1</a>
<a href="https://www.dropbox[.]com/s/EU_adopts_conclusions_on_EU_priorities_in_UN_human_rights_fora_in_2022.zip/?dl=1">https://www.dropbox[.]com/s/EU_adopts_conclusions_on_EU_priorities_in_UN_human_rights_fora_in_2022.zip/?dl=1</a>
<a href="https://www.dropbox[.]com/s/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.dl=1">https://www.dropbox[.]com/s/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.dl=1</a>
<a href="https://uepspr[.]com/2023/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip">https://uepspr[.]com/2023/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip</a>
<a href="https://uepspr[.]com/2023/EU_adopts_conclusions_on_EU_priorities_in_UN_human_rights_fora_in_2022.zip">https://uepspr[.]com/2023/EU_adopts_conclusions_on_EU_priorities_in_UN_human_rights_fora_in_2022.zip</a>

hxxps://www.dropbox[.]com/s/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip/?dl=1	
hxxps://www.dropbox[.]com/s/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.dl=1	
hxxps://uepspr[.]com/2023/EU%20adopts%20conclusions%20on%20EU%20priorities%20in%20UN%20human%20rights%20fora%20in%202022.zip	
hxxps://uepspr[.]com/2023/EU adopts conclusions on EU priorities in UN human rights fora in 2022.zip	
https://upespr[.]com/Council conclusions on the European security situation.zip	
hxxps://45.154.14[.]1235/mfa/Council%20conclusions%20on%20the%20European%20security%20situation.pdf	
hxxp://www.zyber-i[.]com/europa/2022.zip	
hxxps://69.90.184[.]1125/lt/2023.rar	
Council conclusions on the European security situation.exe	6fd9d745faa77a58ac84a5a1ef360c7fc1e23b32d49ca9c3554a1edc4d7618
State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.exe	5851043b2c040fb3dce45c23fb9f3e8aefff48e0438dec7141999062d46c59
Situation at the EU borders with Ukraine.exe	effd63168fc7957baf609f7492cd82579459963f80fc6fc4d261fbc68877f5a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.exe	b2ff5535caa1d70c9d0d59cd68619b142858ae018064c891b4671154aa93a
Advance version of the 2020 Report of the Secretary-General on Peacebuilding and Sustaining Peace.pdf	54b491541376bda85ffb02b9bb40b9b5adba644f08b630fc1b47392625e1e
Council conclusions on the European security situation.pdf	a4ff2c5913cce536759777acee3cfcc8824b927304c8a93ac64d37d1b01a57

Situation at the EU borders with Ukraine.docx	a07cece1fa9b3c813c0b6880b24a6494a9db83e138102da3bce30ebff5190f
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.pdf	0c2f5b6fe538d088fed11ab10925210cb2eb782f471e6f09c484677e82fc5f
State_aid_Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf	ec32ff0c049bd8812a35aeaaaae1f66eaf0ce8aefce535d142862ae89435c2e
PotPlayer.exe	76da9d0046fe76fc28b80c4c1062b17852264348fd873b7dd781f39491f91
FontEDL.exe	19870dd4d8c6453d5bb6f3b2becbbbe28c6f280b6a7ebf5e0785ec386170
PotPlayer.dll	e1dbe58393268d7ddabd4bed0cdef0fbbba85d4c3ef1300580ed4c74e147a
DocConvDll.dll	436d5bf9eba974a6e97f6f5159456c642e53213d7e4f8c75db5275b66fedd
DocConvDll.dll	a01f353c92afcd45b5731815c79f1e1d01366cefa75b41550a28d999857c5
PotPlayer.dll	472822c6bdc710175987eb7d9171f780c974a83ea2b26f117b748babb9b7
PotPlayerDB.dat	fac8de00f031299f6c698b34534d6523428b544aad6a40fdc4b000a04ee82
FontLog.dat	82df9817d0a8dca7491b0688397299943d9279e848cdc4a5446d3159d8d7
FontLog.dat	b9e330373b382beaf4f0bce83d65f13399d42dc3e9fcdc7b4ef26fa893607
PotPlayerDB.dat	03a836034360841fd6b99927c5b639d074e9fce4f16bd4f77ab57a9e5c12d

hxxps://45.154.14[.]235/2023/PotPlayer.exe

hxxps://45.154.14[.]235/2023/PotPlayer.dll

hxxps://45.154.14[.]235/2023/PotPlayerDB.dat

hxxp://103.107.104[.]19/2022/eu.docx

hxxp://103.107.104[.]19/FontEDL.exe

hxxp://103.107.104[.]19/DocConvDll.dll

hxxp://103.107.104[.]19/FontLog.dat

hxxps://69.90.184[.]125/lt/2022.pdf

hxxps://69.90.184[.]125/lt/FontEDL.exe

hxxps://69.90.184[.]125/lt/DocConvDll.dll

hxxps://69.90.184[.]125/lt/FontLog.dat

hxxps://45.154.14[.]235/State\_aid\_\_Commission\_approves\_2022-2027\_regional\_aid\_map\_for\_Greece.pdf

hxxps://45.154.14[.]235/PotPlayer.exe

hxxps://45.154.14[.]235/PotPlayer.dll
hxxps://45.154.14[.]235/PotPlayerDB.dat
hxxp://upespr[.]com/PotPlayerDB.dat
hxxp://upespr[.]com/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf
hxxp://upespr[.]com/PotPlayer.dll
hxxp://upespr[.]com/PotPlayer.exe
hxxps://45.154.14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece.pdf
hxxps://45.154.14[.]235/PotPlayer.exe
hxxps://45.154.14[.]235/PotPlayer.dll
hxxps://45.154.14[.]235/PotPlayerDB.dat
103.107.104[.]19
69.90.184[.]125
45.154.14[.]235

upespr[.]com
www.zyber-ij[.]com
hxtps://92.118.188[.]78

**Emerging Threats Signatures**

2851112    ETPRO TROJAN ta416 Related PlugX Activity (POST)

---

Source: <https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european>